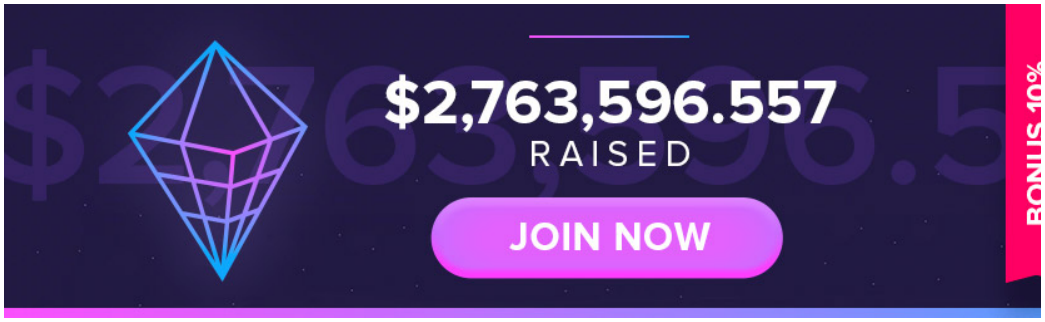
What Is Cryptojacking and How Can You Avoid It?

By **Gavin Phillips** / January 3, 2018 03-01-2018 / 6 minutes

Facebook Twitter Pinterest Stumbleupon Email

Advertisement



A new security threat is in town: cryptojacking. The **cryptocurrency** explosion is moving nefarious individuals to power mining systems anyway possible. And the latest method for securing additional, free power is by hijacking your system resources.

We wrote recently concerning the significant rise in **browser-based cryptocurrency mining scripts**. Well, those scripts are now in their next phase, making it easier for criminals to harvest your machine for longer, without alerting you to the resource-sucking issue at hand.

Gavin Phillips
300 articles

Gavin is the Technology Explained Editor, as well as a Security and Windows regular. He has a Contemporary Writing degree pillaged from the hills of South Devon, but now resides in the deepest depths of Cornwall, calling Penzance his home. In a 10-year writing career he has covered real estate,...

Online adverts are unpopular, so infamous online piracy site The Pirate Bay has hit upon a solution: use every visiting PC to mine cryptocurrencies. Would you be happy if your PC was hijacked like this?

READ MORE

Let's find out what cryptojacking is and what you can do about it.

Why Steal System Resources?

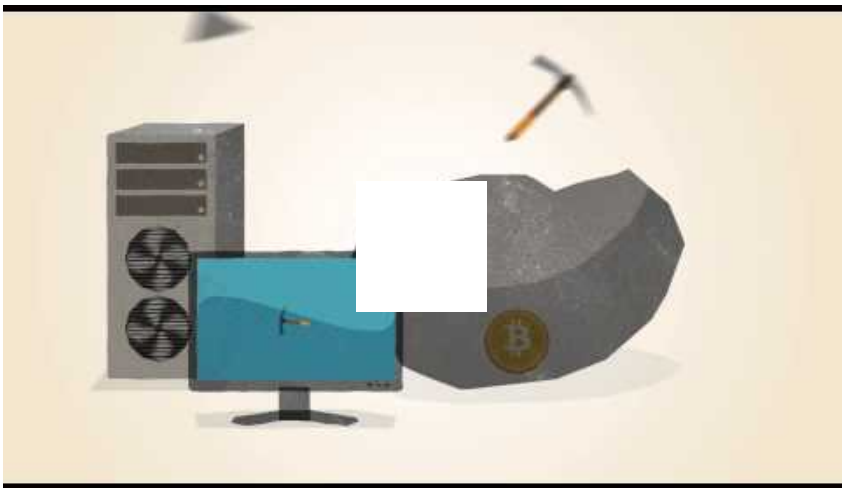
Before we consider cryptojacking as a whole, let's consider the reasons behind it. Why are hackers stealing system resources?

Well, cryptocurrency doesn't grow on trees. No, it grows on servers, waiting to be mined. That doesn't help things, either. The vast majority of **cryptocurrencies use "mining"** to mediate the specific crypto-network.

Is It Profitable to Cloud Mine Bitcoin?

There are many ways to mine **Bitcoin**, including cloud services. But is it profitable? Here's everything you need to know about cloud mining Bitcoin.

READ MORE



Latest Giveaways!

Roccat Sova Review: This is The PC Gaming Lapboard to Buy

Xiaomi Huami Amazfit Bip Review: The Best Fitness Tracker You Can Buy for $100

DJI Does It Again: Mavic Air Review (and Giveaway!)

Trending

SECURITY , INTERNET

5 Popular Firefox Extensions You Should Remove Right Now

PRODUCTIVITY , PROGRAMMING

6 OneNote Tips Programmers Must Try

TECHNOLOGY EXPLAINED

Why Changing DNS Settings Increases Your Internet Speed

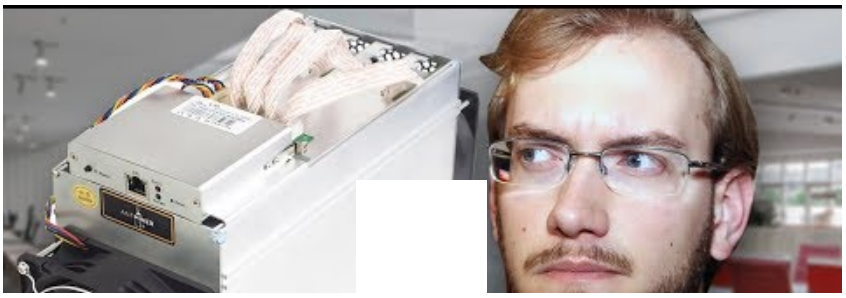
downloaded the blockchain) for verification. The miner's systems process complex equations and, on confirmation that the transactions are legitimate, the block adds to the chain. At that point, the transactions contained in the block process, while the miners receive a block reward (this differs between cryptocurrencies; the current Bitcoin reward is 12.5 **BTC**).

The key to crypto-mining success is how quickly your system processes equations. Bitcoin mining is now useless for the average, nay, even high-end systems. The sheer volume of mining power drowns out tiny home systems. You'll note that if you complete an internet search for "mining pc" the results **all relate to Ethereum** and other, smaller cryptocurrencies.

How to Build an Energy-Efficient Ethereum Mining Rig

Ethereum is an up and coming cryptocurrency. In this article, we cover everything you need to know to build you own mining rig.

READ MORE



Related Articles

SECURITY

How to Stay Safe Online Without the Latest Security Patches

SECURITY

Everything You Need to Know About Bulletproof Hosting Services

INTERNET , SECURITY

Google Account Recovery Won't Work Without This Crucial Step

So, the key to making money mining **cryptocurrency** is raw processing power. And what better way to harness processing power than by stealing that from unsuspecting internet users?

JavaScript Cryptocurrency Mining

That's where cryptojacking picks up the slack. Not content with building mining rigs with expensive specialized equipment, enterprising hackers spotted an opportunity. Cryptocurrency mining scripts aren't *that* new — we've seen several sites trial them as a revenue stream. Furthermore, we've seen several notable websites succumb to cryptocurrency mining.

American TV network Showtime made several public apologies after a crypto-mining script was found concealed on two of their sites. The sites, *Showtime* and *ShowtimeAnytime*, concealed a JavaScript-based Monero miner. The code is developed and maintained by CoinHive, who takes around 30 percent of any block rewards. Showtime neglected to comment on the code, and we are as yet unsure who inserted the code into the sites.

Showtime, however, is far from the only site to feature a JavaScript-based cryptocurrency miner. Ever-present torrenting site The Pirate Bay (**try one of these six alternatives**) experimented with a CoinHive mining script, while Politifact suffered the same issue as Showtime, as did the

Latest Articles

PRODUCT REVIEWS , GAMING

Roccat Sova Review: This is The PC Gaming Lapboard to Buy

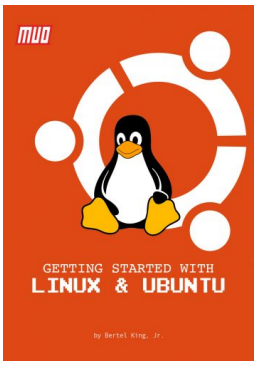
INTERNET

It's Time to Fix Google! How to Bring Back 5 Features It Removed

SOCIAL MEDIA

Why You Should Stop Using Facebook in 2018

Latest Free PDFs



Top 6 Torrent Alternatives to The Pirate Bay

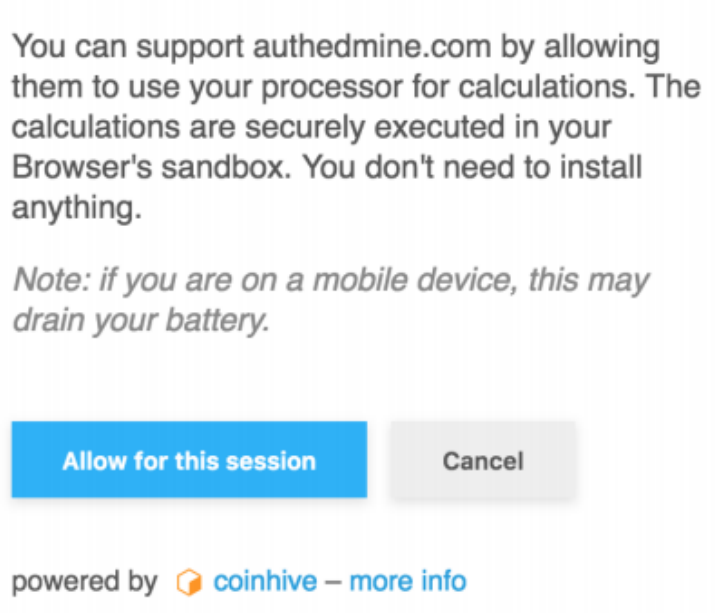
The Pirate Bay shut shop. But there are lots of alternatives out there. You just need to know where to look. Here are the top six torrent sites other than The Pirate Bay.

READ MORE

Okay, So What's Cryptojacking?

Cryptojacking is the coverall term given to this type of drive-by browser-based cryptocurrency mining. CoinHive, purveyors of the most popular script, advertise their product as an alternative to advertising revenue. Their script allows users to "pay you with full privacy, without registering an account anywhere, without installing a browser extension and without being bombarded by shady ads." The last part of that sentence alone is laughable.

The practice has evolved even in the short time CoinHive and its script have been active. The latest version of the script (known as AuthedMine) offers users the chance to accept the cryptocurrency mining, or decline and face regular ads, instead. The new opt-out is optional, mind. Not every website running the CoinHive script will make this offer.

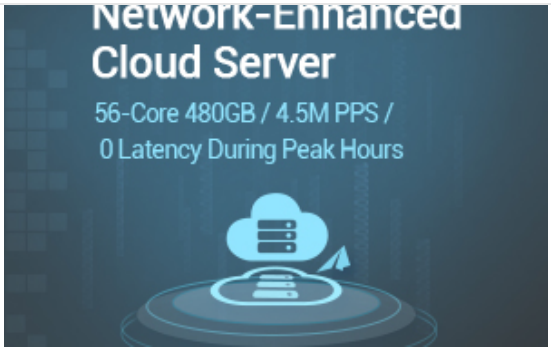


Cryptojacking is evolving in other ways, too. Not content with simply pillaging other people's systems for personal gain, enterprising hackers send unsuspecting users through redirect loops. Users end up on a web page running a cryptocurrency mining script. If they don't notice, hackers make more money.

With that in mind, there are instances of a tiny browser window hiding beneath the system clock, found on the taskbar. The tiny browser window is obscured by the system clock and is "free" to run the mining script until the user notices something is wrong.

How Widespread Is Cryptojacking?

Well, **a recent study** conducted by independent security researcher Willem de Groot revealed 2,496 individual sites running a crypto-mining script. The sites de Groot found all run outdated software that is easily exploited by hackers. A hacker compromises a site then inserts their dedicated CoinHive code, letting the site and its users do the rest.



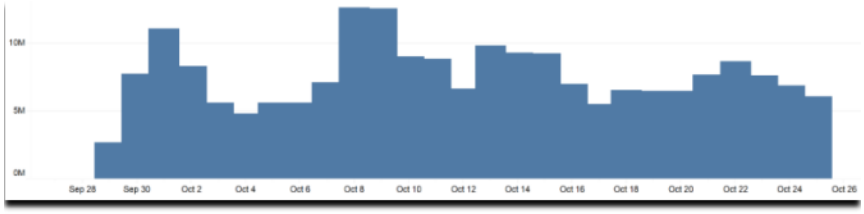
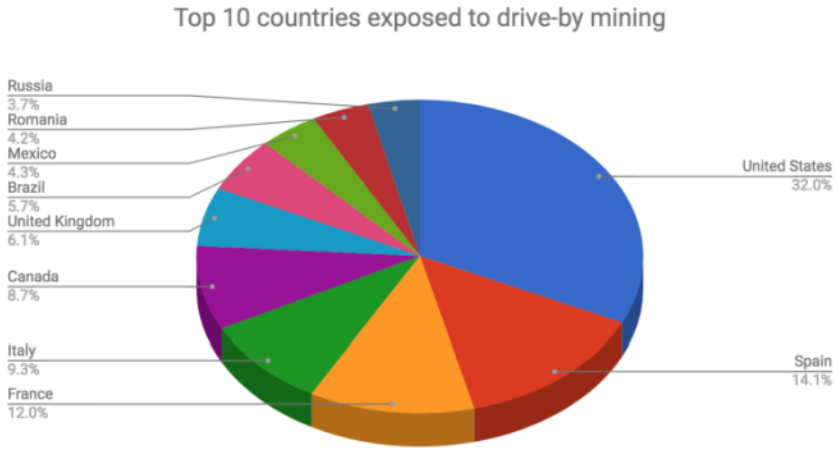


Figure 7: A month worth of blocks for Coinhive's domains and proxies (in millions).

In October 2017, Malwarebytes **reported** [PDF] 8 million blocks *per day*, each preventing potential cryptojacking. Furthermore, the report illustrated cryptojacking activity by geolocation. The U.S. tops the list with 32 percent of all attempted cryptojacking traffic (followed by Spain, France, Italy, and Canada).



Web pages aren't the only thing with the potential for hijacking. Malicious apps are dime-a-dozen on the Google Play Store, but researcher Gabriel Cirlig at ixiacom **noted** two apps with a combined 15 million downloads (both apps have since rectified the issue).

The answer is... it's neither here nor there. Yes, there are malicious apps and websites unwittingly crypto-mining on someone else's behalf. Yes, there are some sites seriously

outlets would have you believe.

Is It Illegal?

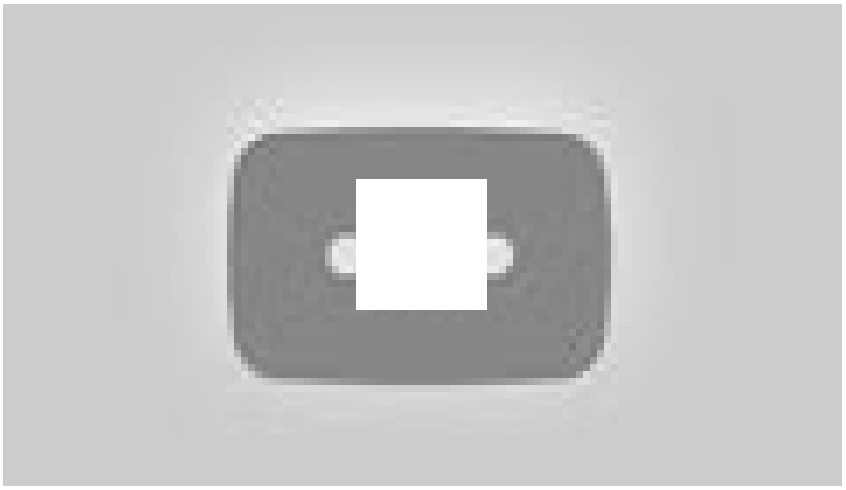
Here's the thing: it isn't illegal — yet. It's only unethical and extremely frowned upon.

But as yet, it isn't illegal to harness someone else's processing power to mine cryptocurrency in this manner. It differs from a botnet because the **hackers are not forcing malware onto your system**. Furthermore, the script itself doesn't create a permanent vulnerability for exploitation by other nefarious parties. When the tab closes, the miner stops.

The Complete Malware Removal Guide

Malware is everywhere these days, and eradicating malware from your system is a lengthy process, requiring guidance. If you think your computer is infected, this is the guide you need.

READ MORE



The serious complications arise because to some, CoinHive and "legitimate" browser-based crypto-mining scripts present a viable, even attractive alternative to the bloated advertising networks. As advertisers become more aggressive in their ad displays, more and more people are switching ad-blockers on.

anyway. (**Malvertising campaign, anyone?**)

Major institutions are unsure how to approach it, too. Malwarebytes blocks the CoinHive site as a malicious or unwanted site. But Malwarebytes Lab director Adam Kujawa says, "I actually think the whole concept of a script-based miner is a good idea. It could be a viable replacement for something like advertising revenue. But we're blocking it now just because there's no opt-in option or opt-out. We've observed it putting a real strain on system resources. The scripts could degrade hardware."

Unfortunately for CoinHive, intentions good or bad, their original script is out there. And that script is popping up again and again in less-than-favorable circumstances, on websites that are obviously compromised.

How Do I Stay Safe?

Staying safe isn't actually too difficult. There are two main methods.

1. **Browser Extensions:** There are several anti-mining specific extensions for Chrome (the browser with the highest rate of cryptojacking). Try **No Coin** or **minerBlock**.
2. **Script Blockers:** The above blockers focus on mining scripts. There are other excellent script blockers available for Chrome and other browsers. **uBlock Origin** has an excellent array of script blocking lists. Mozilla users might try **NoScript**.

As we have seen, cryptojacking isn't an enormous problem — yet. But as more sites realize it is a potentially lucrative revenue stream there may well be an uptick.

Have you experienced cryptojacking? What site were you visiting? Did you realize straight away? What do you think about cryptojacking as a standard advertisement replacement? Let us know your thoughts in the comments!

joining our newsletter!

your@email.com Submit

2 COMMENTS WRITE A COMMENT

Main Sale ends in: The Revolution!

© 2018 MakeUseOf. All Rights Reserved.